Organizational Narrative

IronHub Inc

August 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.2, CC1.3, CC1.4, CC1.5, CC3.1, CC3.2, CC3.3

Table 2: Document history

Date	Comment
Apr 1 2022	Initial document

Date	Comment
Apr 21 2026	Updated to reflect current organizational structure and Canadian corporate context

1 Organizational Narrative

The following provides a description of the corporate and management structure of IronHub.

The intent of this description is to establish both the legal jurisdiction and corporate cultural norms that serve as the foundation for IronHub's compliance program.

2 Entity Type

IronHub is an Alberta Corporation headquartered in Calgary, Alberta, Canada. IronHub was founded and incorporated in October 2015.

3 Integrity and Ethics

The Directors and Executives of IronHub aspire to and demonstrate standards of ethics and integrity consistent with professional norms in Canadian corporate environments.

Chief among these standards is a commitment to honesty in interactions with and among managers, directors, employees, contractors, customers, and other stakeholders. These standards are codified in IronHub's Code of Conduct Policy, which all employees and contractors are required to acknowledge annually.

4 Board Independence

The Board of Directors appoints and oversees the Chief Executive Officer (CEO). The Board provides independent oversight of management's performance and strategic direction.

5 Organizational Structure

IronHub is composed of the following primary divisions:

- Sales
- Marketing
- Client Services & Support
- Research & Development
- Information Technology
- Human Resources
- Finance

Each division is led by a Vice President, who in turn reports to the CEO. A complete Organization Chart is maintained and distributed by Human Resources.

6 Management Objectives

Work is distributed to each division via Objectives set by the respective division Vice President, in collaboration with the Chief Executive Officer. Objectives are reviewed and updated on a regular cadence to align with company strategy and evolving risk.

7 Risk to Objectives

IronHub seeks to manage risk to Objectives through professional management strategies and tactics, including:

- Rigorous hiring practices including background checks
- Employee performance reviews
- Aligning compensation with objectives
- Regular communication of objectives by executive management
- Annual risk assessments conducted by the Information Security Manager (ISM)

8 Fraud Risk to Objectives

IronHub acknowledges the possibility that fraud may imperil corporate objectives. IronHub undertakes various activities to manage fraud risk, including:

- Conducting regular financial audits
- Adhering to financial control principles including segregation of duties
- Investigating suspicious transactions
- Performing criminal background checks on all employees
- Maximizing the use of information technology in fraud detection
- Maintaining cyber insurance coverage for cyber crime events including funds transfer fraud and social engineering

9 Security Awareness and Training

IronHub maintains a security awareness training program to ensure all personnel understand their responsibilities for protecting information assets. All employees and contractors must complete foundational security awareness training within 5 business days of starting and annual refresher training thereafter. Role-based training is provided to developers, system administrators, and executives based on their specific risk exposure.

10 Compliance Oversight

The Information Security Manager (ISM) is responsible for overseeing IronHub's compliance program, including maintenance of policies, coordination of audits, and management of the risk assessment process. The ISM reports compliance status to the Leadership Team on a quarterly basis.